Article 34 Amendment

CLAIMS

1. A method of providing a value note comprising:

providing first information representative of public key information for a bearer, or from which public key information for a bearer can be verified;

providing second information representative of a commodity represented by the value note; and

calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of public key information for the issuer.

2. A method according to claim 1, wherein the first information represents public key information for the bearer.

3. A method according to claim 1 ~~or 2,~~ further comprising providing information on when the value note is due to expire.

4. A method according to claim 3, wherein the expiry information is included in the calculation of the signature.

5. A method according to claim 1, ~~2, 3 or 4~~, further comprising providing identification information for uniquely identifying the value note.

6. A method according to claim 5, wherein the identification information comprises a serial identification string.

7. A method according to claim 5 ~~or 6~~, wherein the identification information is included in the calculation of the signature.

8. A method according to ~~any preceding~~ claim 1, further comprising providing valid-from information representing from when the value note is available for redemption.

9. A method according to claim 8, wherein the valid-from information is included in the calculation of the signature.

AMENDED SHEET

10. A method according to ~~any preceding~~ claim 1, further comprising communicating the value note electronically.

11. A method according to claim 10, wherein the value note is sent through an electronic public communication system.

12. A method according to ~~any preceding~~ claim 1, wherein the issuer's signature is an RSA type signature.

13. A method of handling a value note, comprising:

receiving a value note comprising first information representative of a bearer's public key or from which bearer's public key can be verified, second information representative of a commodity represented by the value note, and third information representing an issuer's signature which can be verified by information including the first and second information and public key information for the issuer;

providing redemption instruction information for the value note; and

providing a bearer's signature which is dependent on the payment instruction information and is verifiable from said first information.

14. A method according to claim 13, wherein the bearer's signature is an RSA type signature.

15. A method according to claim 13 ~~or 14~~, wherein the value note is as provided by the method or any of claims 1 to 12.

16. A method according to claim 13, ~~14 or 15~~, wherein the step of providing the bearer's signature comprises calculating the signature based on information including the redemption instruction information and a secret key related to the first information.

17. A method according to claim 16, wherein said information on which the bearer's signature is calculated includes information from the value note.

AMENDED SHEET

18. A method according to claim 13, ~~14, 15, 16 or 17~~, wherein the redemption instruction information includes a reference to transfer at least a proportion of the commodity to a first new value note.

19. A method according to claim 18, wherein the redemption instruction information includes replacement first information for the new value note.

20. A method according to claim 18 ~~or 19~~, wherein the first new value note has a different bearer's public key from the value note being redeemed.

21. A method according to claim 18, ~~19 or 20~~, wherein the redemption instruction information includes a reference to transfer the or a remainder of the commodity to a second new value note.

22. A method according to claim 21, wherein the second new value note has a different bearer's public key from the value note being redeemed.

23. A method according to claim 18, ~~19, 20, 21 or 22~~, wherein the redemption instruction information includes a reference to transfer the commodity represented by the first new value note to a replacement new value note if the first new value note is not redeemed within a predetermined period.

24. A method according to claim 23, wherein the replacement new value note has a ~~different bearer's public key from the first new value note.~~

25. A method according to ~~any of claims 13 to 24~~ claim 13, wherein the instruction information includes an identification reference for the or each value note referred to in the instruction information, and wherein the method comprises communicating the instruction information to a value note handling authority.

26. A method according to ~~any of claims 13 to 25~~ claim 13, further comprising communicating the value note, the redemption instruction information and the bearer's signature information to a value note handling authority.

AMENDED SHEET

27. A method according to claim 25 ~~or 26~~, wherein the communication is effected over an electronic public communication system.

28. A method of handling redemption instruction information and bearer signature information associated with a value note, the method comprising performing at least one verification prior to redeeming the value note in accordance with the redemption instruction information, the verification comprising:

verifying that the bearer signature information matches information including at least the payment redemption instruction information using public key information for the bearer presented in the value note or in the instruction redemption information.

29. A method according to claim 28, wherein the redemption instruction information is associated with a plurality of value notes.

~~30. A method according to claim 28, wherein the instruction redemption information is provided by the method of any of claims 13 to 27.~~

31. A method according to claim 28, ~~29 or 30~~, wherein the redemption instruction information and the bearer signature information are received without a value note, and the method comprises retrieving value note information for one or more value notes identified in the instruction redemption information.

32. A method according to ~~any of claims 28 to 31~~ claim 28, further comprising verifying that an issuer signature included in the value note matches information including the bearer public key information and the commodity represented by the value note, using public key information for the issuer.

33. A method according to ~~any of claims 28 to 32~~ claim 28, further comprising verifying that the value note has not previously been presented for redemption.

34. A method according to ~~any of claims 28 to 33~~ claim 28, further comprising verifying that the value note has not previously been redeemed validly.

AMENDED SHEET

35. A method according to claim 33 ~~or 34~~, wherein the value note and/or the redemption instruction information includes identification information for uniquely identifying the value note, and the verification comprises ascertaining whether a value note bearing the same identification information has previously been accepted.

36. A method according to ~~any of claims~~ claim 28 ~~to 35~~, further comprising verifying whether a counter signature matches public key information in the value note for a counter signatory.

37. A method according to ~~any of claims 28 to 36~~, further comprising verifying whether an endorsement signature in the value note matches information including a predefined message using public key information for the message endorsing signatory.

38. A method according to ~~any of claims 28 to 37~~, wherein the value note includes expiry time and/or date information representing a time and/or date of expiry, and the method further comprises testing the value note on the basis of the expiry information.

39. A method according to ~~any of claims 28 to 38~~, wherein the value note includes valid-from time and/or date information representing a time and/or date from which the value note may validly be redeemed, and the method further comprises testing the value note on the basis of the valid-from information.

40. A method according to ~~any of claims 28 to 39,~~ wherein the step of redeeming the value note comprises issuing a first new value note representing at least a proportion of the commodity of the value note being redeemed.

41. A method according to claim 40, wherein first new value note includes different public key information from the value note being redeemed.

42. A method according to claim 40 ~~or 41~~, wherein the step of redeeming the value note comprises issuing a second new value note representing the or a remainder of the commodity of the value note being redeemed.

AMENDED SHEET

43. A method according to claim 42, wherein the second new value note includes a different bearer public key from the value note being redeemed.

44. A method according to claim 40, ~~41, 42 or 43~~, wherein the step of redeeming the value note comprises issuing a replacement new value note if said first new value note is not redeemed within a predetermined period.

45. A method according to claim 44, wherein the replacement value note includes a different bearer's public key from the value note being redeemed.

46. A method according to ~~any of claims 40 to 45~~ claim 40, wherein at least one new value is issued which includes information indicative of a time and/or date from which the new value note can be redeemed, and wherein the time and/or date is later than the time and/or date, respectively, of issuance.

47. A method according to ~~any of claims 28 to 46~~ claim 28, further comprising communicating the or each new value note electronically to a remote party corresponding to the source of the value note being redeemed.

48. A method according to claim 47, wherein the communication is effected over a public communication system.

49. A method wherein an electronic representation of a commodity is issued by an issuing authority, the electronic representation including information representing a time and/or date from which the electronic representation is available for redemption, said time and/or date being later than the time and/or date of issuance, whereby the electronic representation is not available for redemption immediately after issuance.

50. A method according to claim 49, wherein the commodity is money.

51. A method according to claim 18 ~~or to any claim dependent thereon~~, wherein the method comprises generating a first character string message, generating a second character string

AMENDED SHEET

message from said first message in the redemption instruction information for inclusion in the new value note.

52. A method according to claim 51, further comprising the steps of:

communicating the value note, the redemption instruction information, and the bearer's signature information to a value note handling authority;

issuing a new value note including the blinded second character string message, in accordance with the redemption instruction information;

communicating the new value note to a respondent; and

providing endorsement signature information from the respondent dependent on the first and second character string message and related to the blinding function such that the endorsement signature is verifiable against both the first character string message and the second character string message; and

communicating the value note and the respondent's endorsement signature information to the value note handling authority.

53. A method according to claim 52, further comprising the step of unblinding the second character string message by the respondent to yield the first character string message prior to providing the respondent's endorsement signature information.

54. A method of encrypting data, comprising:

applying a blinding function to encrypt said data using first secret key information;

calculating a digital signature using a signature function which is dependent firstly on said blinded data or on blinded hashing information calculated from unblinded data, and secondly on second secret key information, in such a manner that the signature is verifiable using public key information related to the second secret key;

composing a message including the encrypted data, the digital signature, and encrypted information relating the first secret key;

whereby it is possible to verify from said encrypted data and from said digital signature that the signature matches the encrypted data without decrypting the encrypted data, and whereby, with knowledge of the encryption used to encrypt the first secret key information in the message, it is possible to ascertain the first secret key information and to decrypt said encrypted data.

AMENDED SHEET

55. A method of encrypting and transmitting data, comprising:

applying a blinding function to the data to encrypt said data using first secret key information;

composing s first message including the encrypted data and encrypted information relating to the first secret key;

transmitting the first message to a first receiver;

calculating a digital signature using a signature function which is dependent firstly on said blinded data or on blinded hashing information for the blinded data, and secondly on second secret key information, in such a manner that the signature is verifiable using public key information related to the second secret key;

composing a second message including the encrypted data, the encrypted information relating to the first secret key and the digital signature;

transmitting the second message to a second receiver.

56. A method according to claim 55, further comprising calculating said hashing information for the unblinded data and including said hashing information in the first message.

57. A method according to claim 55 ~~or 56~~, further comprising the following steps after receipt of the first message by the first receiver:

de-crypting the encrypted information relating to the first secret key; and

un-blinding the encrypted data using the de-crypted first secret key information.

58. A method according to claim 55, ~~56 or 57~~, further comprising the following step after receipt of the second message by the second receiver:

verifying whether the digital signature matches the encrypted data.

59. A method comprising:

(a) a first method as defined in any of claims 1 to 12 or 51; and

(b) a second method as defined in any of claims 13 to 27.

60. A method according to claim 59, further comprising a third method as defined in any of claims 28 to 48.

AMENDED SHEET

61. A value note comprising:

first information representative of public key information for a bearer, or from which public key information for a bearer can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

62. A record carrier on which is recorded value note information including:

first information representative of public key information for a bearer, or from which public key information for a bearer can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

63. A transmission signal representing a value note and comprising:

first information representative of public key information for a bearer, or from which public key information for a bearer can be verified;

second information representative of a commodity represented by the value note; and

third information representative of an issuer's signature which is verifiable from information including the first information, the second information and public key information for the issuer.

64. A value note as defined in claim 61, or a record carrier as defined in claim 62, or a signal as defined in claim 63, further comprising identification information for uniquely identifying the value note.

65. A method of providing redemption instruction information for one or more value notes each being as defined in claim 64, the method comprising:

providing a list of identification information for identifying each existing value note to be used in the transaction;

AMENDED SHEET

providing a list of redemption requests, each request including information representing a result of the transaction, and a commodity value associated with that result;

providing a signature information representing a bearer's signature which is verifiable from the information in the instruction and/or from information in said value notes, and public key information for the bearer.

66. A method according to claim 65, wherein at least one redemption request includes a request to issue a new value note.

67. A method according to claim 65 ~~or 66~~, further comprising providing information representing public key information for the bearer.

68. A method according to claim 65, ~~66 or 67~~, further comprising providing information representing the total value of the existing value notes, which total value is to divided or allocated in accordance with the list of redemption requests.

69. A method according to claim 65, ~~66, 67 or 68~~, further comprising communicating the instruction information, with or without the individual value notes referred to in the instruction information, to a money handling authority.

70. A method as defined in any of claims 1 to 60 or 65 to 69, or a value note as defined in claim 61, or a record carrier as defined in claim 62, or a transmission signal as defined in claim 63, wherein the information representing the value represents a fixed absolute value.

71. A method as defined in any of claims 1 to 60 or 65 to 69, or a value note as defined in claim 61, or a record carrier as defined in claim 62, or a transmission signal as defined in claim 63, wherein the information representing the value defines a formula representing a variable value.

72. A method as defined in any of claims 1 to 60 or 65 to 69, or a value note as defined in claim 61, or a record carrier as defined in claim 62, or a transmission signal as defined in claim 63, wherein the information representing the value represents a fixed or variable value by reference to an identifying label.

AMENDED SHEET

73. An electronic representation of a commodity, the representation including first time and/or date information representing a time and/or date up to which the electronic representation is guaranteed, and second time and/or date information representing a time and/or date later than the first time and/or date and up to which the electronic representation may still be valid but without a guarantee.

74. Apparatus for carrying out a method as defined in ~~any of claims 1 to 60, or 65 to 72~~ claim 1.

AMENDED SHEET